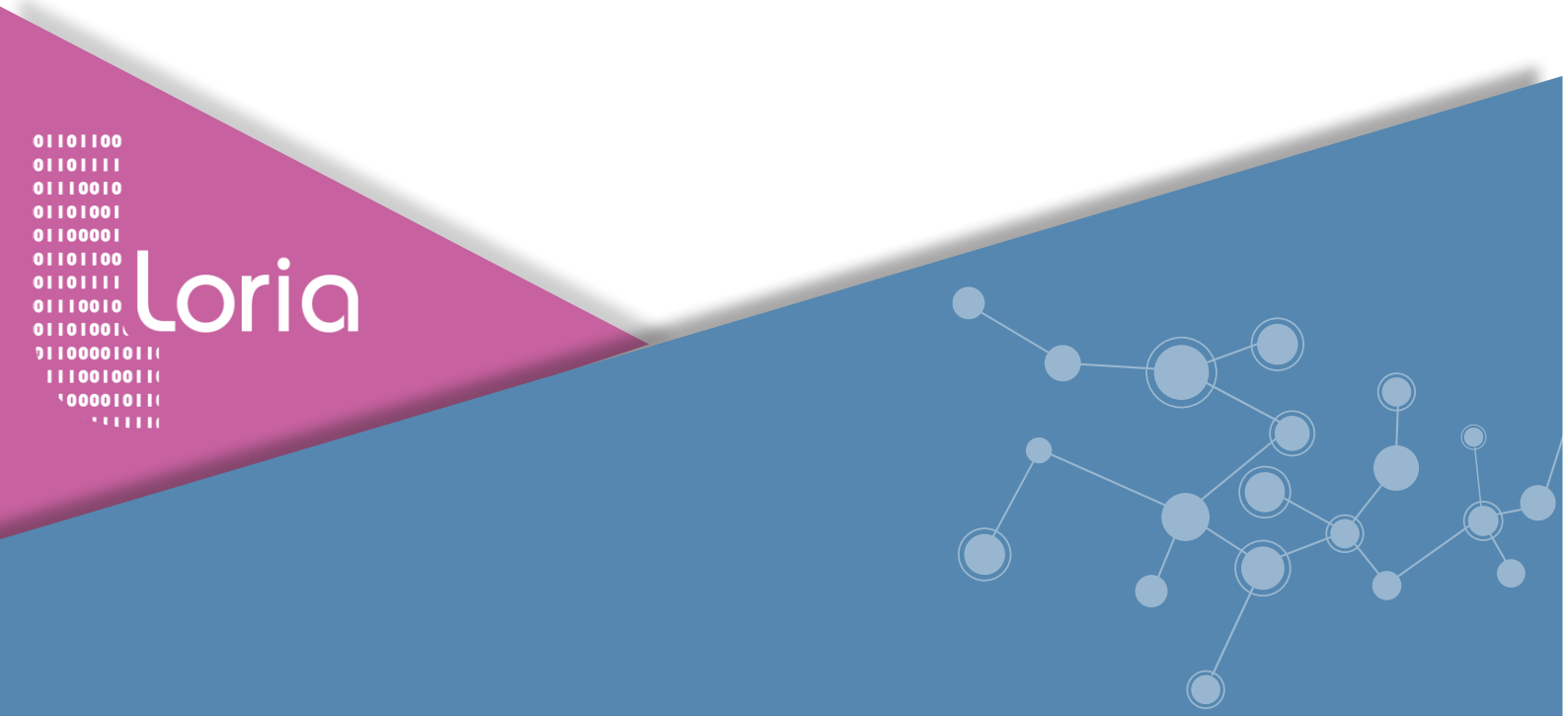
Département
D2: Formal Methods

Équipe Team Carbone

Computer science beyond the realm of reason



Laboratoire lorrain de recherche en informatique et ses applications

Rapport d'activité 2025

En partenariat avec

Contents

Team Carbone

Keywords

Cybersecurity, Malware, Implicit Computational Complexity

1 Team members, visitors, external collaborators

Faculty Members

- Jean-Yves Marion [Team leader, Université de Lorraine, Professeur, HDR]
- Guillaume Bonfante [Université de Lorraine, Maitre de conférences, HDR]

Post-Doctoral Fellows

- Florent Martin [INRIA, Post-Doctoral Fellow, until Mar. 2025]

PhD Students

- Gabriel Sauger [UL, PhD Student]
- Quentin Jacqmin [UL, PhD Student]
- Vidal Attias [UL, PhD Student]
- Léo Bertrand [UL, PhD Student]
- Sébastien Larinier [UL, PhD Student]

Technical Staff

- Maira Nassau [INRIA, Engineer, since 2023]
- Pierre Marty [INRIA, Engineer, since 2023]
- Romain Guittienne [INRIA, Engineer, since 2023]

Interns and Apprentices

- Victor Matrat [UL, Intern, until Aug. 2025]

Administrative Assistant

- Elsa Maroco [UL]

External Collaborators

- Eric Freyssinet [Gendarmerie Nationale]

2 Overall objectives

The Carbone team's research focuses on malware and all its interactions: systems, networks, criminal ecosystems and so on.

Three main objectives have been set:

Defence against malware

- Analysis and reverse engineering of malware using white-box (DSE) and black-box (program synthesis, grammatical inference) approaches.
- Detection of malicious behaviour
- Forensics

Understanding offensive tactics

- Adversarial example and supply chain attack
- Building an attack chain

An interdisciplinary approach to the study of malicious ecosystems

- The study of organisations and communications
- The study of underground economies

As a secondary objective, we keep an activity in the domain of (implicit computational) complexity and program analysis.

3 Research program

3.1 Compréhension-Détection-Analyse Forensique des Malwares

Le premier sujet de recherche s'articule autour des trois axes Compréhension-Détection-Analyse Forensique. La lutte contre les malwares nécessite de développer de nouvelles heuristiques. Pour cela, il est nécessaire d'avoir des outils de rétro-ingénierie pour comprendre l'intention d'un programme, trouver des compromissions/backdoors de composants matériels et logiciels. Et si l'attaque a réussi, il faut avoir des outils d'analyse forensique pour caractériser l'attaque en vue d'une éventuelle attribution par les acteurs en charge. Pour atteindre ce premier objectif et ainsi augmenter significativement le niveau des défenses, le défi est de dépasser l'état de l'art actuel en combinant méthodes formelles, rétro-ingénierie et apprentissage automatique (IA).

3.2 Ecosystème complet du malware

Le second sujet est la compréhension et la documentation de « l'écosystème complet du malware ». Au-delà des aspects techniques, il est important d'appréhender les aspects économiques, juridiques, criminels et sociologiques qui sous-tendent cet écosystème. Pour cela, il est impératif d'avoir une approche interdisciplinaire avec un dialogue et des rencontres/assises. En complément de cette cartographie, le dernier défi est de se doter d'instrument de prédiction et de prévention des modes opératoires, des nouvelles cibles ou encore des nouveaux modes d'organisation.

3.3 Complexité Implicite des Caluls

Le troisième sujet est l'étude de ce qui est calculable en prenant en compte des contraintes physiques comme le temps et l'espace. Ce travail est aujourd'hui fait en collaboration avec l'équipe Mocqua et porte sur la complexité de type 2.

4 Application domains

Les travaux réalisés dans l'équipe sont employés en cyber-sécurité. De nombreuses entreprises ou institutions publiques sont impliquées dans les travaux de l'équipe.

L'équipe Carbone participe au projet DefMal (PEPR Cybersecurity – France 2030 – ANR).

5 Social and environmental responsibility

Le travail d'Eric Freyssinet dans l'équipe témoigne de l'apport de l'équipe.

Nous participons également à l'évènement CyberHumanumEst, une cyber-guerre organisée conjointement entre l'Université de Lorraine et le COMCYBER.

La vie de l'équipe est rythmée par des réunions hebdomadaires destinées au suivi des activités de recherche, ainsi que par nos conférences du club et nos webinaires DefMal.

6 New software, platforms, open data

6.1 BOA

BOA is a binary analysis tool based on symbolic execution. We can solve certain obfuscations and thus be close to dynamic analysis results without executing the binary.

To evade detection, malware developers implement various software protections, called obfuscations, to hide sensitive code. These obfuscations include self-modification, which involves executing code not present in the original binary, which particularly hinders static analysis. State-of-the-art tools use dynamic analysis to circumvent these protections. However, dynamic analysis requires stealthy-enough tools in a secure environment, which is hard to achieve.

6.2 Goatracer

GoaTracer is a hybrid dynamic binary analysis platform combining instrumentation and introspection to efficiently reconstruct Control Flow Graphs and Call Graphs of Windows Portable Executable files. GoaTracer minimizes execution slowdowns, tracks obfuscated and self-modifying code, and bypasses anti-analysis measures, offering a comprehensive view of malware behavior.

7 New results

7.1 Implicit computational complexity

Participants: Jean-Yves Marion.

The class of Basic Feasible Functionals BFF is the second-order counterpart of the class of first-order functions computable in polynomial time. We present several implicit characterizations of BFF based on a typed programming language of terms. These terms may perform calls to non-recursive imperative procedures. The type discipline has two layers: the terms follow a standard simply-typed discipline and the procedures follow a standard tier-based type discipline. BFF consists exactly of the second-order functionals that are computed by typable and terminating programs. The completeness of this characterization surprisingly still holds in the absence of lambda-abstraction. Moreover, the termination requirement can be specified as a completeness-preserving instance, which can be decided in time quadratic in the size of the program. As typing is decidable in polynomial time, we obtain the first tractable (i.e., decidable in polynomial time), sound, complete, and implicit characterization of BFF, thus solving a problem opened for more than 20 years.

7.2 Aspects offensifs

Participants: Leo Bertrand, Maira de Freitas Pereira, Jean-Yves Marion.

Les capacités offensives de l'intelligence artificielle dans le cyberespace L'objectif de l'agent autonome M32 est d'infiltrer une entreprise de haute technologie ; il embarque les dernières mises à jour et peut être considéré comme un des Systèmes d'Armes Cyber Autonomes (SACA) les plus avancés. Il analyse rapidement des millions de documents en accès libre sur internet pour identifier les meilleurs vecteurs de compromission initiale. Les motifs de mots de passe utilisés et partagés avec des proches d'un ingénieur de l'entreprise semblent être la piste statistiquement la plus prometteuse. Furtivement, M32 s'introduit ainsi dans le système de l'entreprise ciblé. Il utilise les fonctionnalités du système, lance les contre-mesures nécessaires pour éviter toute détection et installe des portes dérobées (backdoors).

7.3 Aspects offensifs

Participants: Guillaume Bonfante.

We propose a new framework for the analysis of program execution, devoted to identifying cryptographic functions and retrieving cryptographic secrets. The need for a new tool arises from our experimental observation that the generic analysis tools are clearly too intrusive / resource-consuming for the inspected process, leading to failures such as timeouts. Thus our aim is to build dynamic monitoring tools as lightweight as possible to inspect the execution of sensitive code without impacting the execution.

8 Bilateral contracts and grants with industry

9 Partnerships and cooperations

9.0.1 Visits of international scientists

Mizuhito Ogawa, chercheur au JAIST – Kanazawa – Japon, a rencontré l'équipe en décembre 2025.

9.0.2 Visits to international teams

Jean-Yves Marion est allé à de nombreuses reprises au Japon (JAIST), à Taiwan (Taipei) et au Vietnam (Hanoi) dans le cadre du projet Defmal. Il est également impliqué dans plusieurs consortiums européens (e.g. Europol).

Guillaume Bonfante a rendu visite à Marc Frappier, à l'Université de Sherbrooke, Canada au mois de juin 2025.

Victor Matrat a passé une partie de son stage à l'Université d'Arizona.

9.1 National initiatives

Jean-Yves Marion est responsable du projet Defmal, un projet de l'ANR.

10 Dissemination

Member of the conference program committees Guillaume Bonfante participe au comité de programme de FPS et de .

Jean-Yves Marion participe au comité de programme d'ESORICS, de FPS, de Botconf.

Reviewer

10.0.1 Scientific expertise

Jean-Yves Marion est membre du comité scientifique de l'ANSSI.

10.0.2 Research administration

Jean-Yves Marion est responsable du programme DEFMAL.

10.1 Teaching - Supervision - Juries

Guillaume Bonfante a supervisé les projets de fin d'étude de 2 étudiants en master. Jean-Yves Marion a supervisé les projets de fin d'étude de 2 étudiants en master.

10.1.1 Teaching

- Guillaume Bonfante est responsable de l'option de cyber-sécurité aux Mines de Nancy, France.

10.1.2 Supervision

Jean-Yves Marion est responsable de 4 thèses.
Guillaume Bonfante est responsable de 1 thèse.

10.1.3 Juries

Jean-Yves Marion a été rapporteur de 5 thèses.

10.2 Popularization

Léo Bertrand, Maira Nassau et Jean-Yves Marion ont proposé un article au Études françaises de renseignement et de cyber, Presse Universitaires de France

10.2.1 Education

Guillaume Bonfante et Jean-Yves Marion sont enseignants à l'Ecole des Mines. Guillaume Bonfante est responsable de deux cours de master à la FST, Université de Lorraine.

10.2.2 Interventions

Jean-Yves Marion participe à de nombreuses interventions, comme à Botconf, aux journées de l'AFSIN, à Europol.

11 Scientific production

11.1 Major publications

[1] G. Bonfante. 'The virology of information systems in the power grid'. In: *The Palgrave Handbook on Cybersecurity, Technologies and Energy Transitions*. Ed. by A. Barichella and J. Yada. Palgrave Studies in Energy Transitions. Palgrave Macmillan, 2025. DOI: 10.1007/978-3-031-04196-9_4-1. URL: https://hal.science/hal-05017720.

[2] E. Hainry, B. M. Kapron, J.-Y. Marion and R. Péchoux. 'Complete and tractable machine-independent characterizations of second-order polytime'. In: *Logical Methods in Computer Science* Volume 21, Issue 1 (Jan. 2025). DOI: 10.46298/lmcs-21(1:5)2025. URL: https://inria.hal.science/hal-05097335.

11.2 Publications of the year